



**London School of Economics
& Political Science
IMT**

Policy

Encrypted Authentication

Jethro Perkins
Information Security Manager

Version	1.1
Date	18/03/2015
Library reference	ISM-PY-127

Document control

Distribution list

Name
Information Security Advisory Board
Information Technology Committee

External document references

Title	Version	Date	Author
Information Security Policy	3.1	08/07/13	Jethro Perkins

Version history

Date	Version	Comments
26/01/15	0.1	Initial draft
28/01/14	0.2	Incorporated comments from Chris Roberts. Release to ISAB.
09/03/15	1	Release to ITC
18/03/15	1.1	Updated following ITC comments

Review control

Reviewer	Section	Comments	Actions agreed
ISAB ITC	3	No changes requested It was pointed out that the Policy 'as is' would render us non-compliant. An alteration was requested to indicate how we would approach services that were still sending user authentication details in clear text	Section 3 updated accordingly. 'Legacy systems' section added.

Table of contents

1	Introduction	4
1.1	Purpose	4
1.2	Scope	4
2	Responsibilities.....	5
3	Policy.....	6
3.1	User Authentication	6
3.2	Acceptable Methods.....	6
3.3	Deprecated algorithms and protocols	6
3.4	Legacy Systems	6
3.5	Review and Development	6

1 Introduction

Unencrypted methods of authentication are a major threat to the security of user credentials, and consequently to the confidentiality, integrity and availability of LSE information. They allow usernames and passwords to be passed in clear text, making it a trivial matter to intercept account credentials and use them to gain unauthorised access to LSE resources. At the time of writing this policy, there are still some applications within LSE that use cleartext authentication legacy, presenting an unacceptable risk of exposure to LSE's user community.

1.1 Purpose

This policy will provide a basis from which to ensure that all methods of authentication across LSE applications and systems takes place using encryption.

1.2 Scope

All systems and applications developed by LSE or used by LSE (even if developed by third parties and hosted offsite) that require users to authenticate their identity by the input of a username and password.

2 Responsibilities

Application Developers

Ensuring that all applications requiring username and password authentication do so using encryption.

Project Manager

Ensuring any project to implement an application that requires username and password authentication does so using an encrypted method.

IMT Information Security Manager

Review of all project mandates and business cases. Technical review of authentication measures as appropriate. Requesting redesign / reimplementation as necessary of any application in order to achieve compliance with this policy. Requesting removal or remediation plan for any non-compliant application. Management of LSE's interface with Janet certificate service.

IMT Systems

Requesting and installing as necessary SSL certificates from Janet. Alerting Information Security Manager of any noncompliance with this policy.

IMT Networks

Providing encrypted site-to-site transport and other remedial measures as appropriate.

3 Policy

3.1 User Authentication

All user authentication (i.e. the input of a username and password in order to gain access to a system or application) must be protected by an encrypted protocol, in order to ensure that username and password details are not passed in clear text.

3.2 Acceptable Methods

By default, applications requiring user authentication should use the encrypted version of protocols, for instance:

- FTPS or SFTP rather than FTP
- HTTPS rather than HTTP
- NLA for remote desktop connections
- Encrypted POP3 or POP3S
- SMTPS rather than SMTP

Otherwise, cleartext protocols handling user authentication must be tunnelled via an encrypted protocol (e.g. SSH).

SSL certificates purchased via Janet will by default provide an acceptable level of encryption for web forms requiring user authentication.

3.3 Deprecated algorithms and protocols

Known weak encryption algorithms and vulnerable protocols must not be used in *new* implementations. These include, but are not restricted to:

Algorithms

- DES
- RC4
- SHA-1 in SSL Encryption

Protocols

- SSLv3
- NTLM

3.4 Legacy Systems

It may be impossible for some legacy systems to comply with this policy. In such cases, where legacy systems are identified that use no encryption or deprecated algorithms and protocols, a plan for mitigation or remediation will be put in place.

3.5 Review and Development

This policy, and any subsidiaries, shall be reviewed by the Information Security Advisory Board (ISAB) and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

Additional regulations may be created to cover specific areas.

The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems